

Comments by the Centre for Information Policy Leadership on the European Data Protection Board's draft Guidelines 10/2020 on restrictions under Article 23 GDPR

The Centre for Information Policy Leadership (CIPL)¹ welcomes the opportunity to respond to the European Data Protection Board (EDPB)'s draft guidelines 10/2020 on restrictions under Article 23 GDPR² (Guidelines). The Guidelines are key to clarify the safeguards that apply, the relevant criteria to consider and the assessments to perform when the rights of individuals may be restricted under the GDPR.

1. Executive Summary

The EDPB's Guidelines are aimed at EU Member States and, to a lesser extent, Data Protection Authorities (DPAs). The Guidelines only occasionally refer to the role of controllers.³ There is a danger that the Guidelines will conflate the roles of Member States in setting restrictions under Article 23, of DPAs in supervising the application of restrictions in accord with Member State law and of controllers in applying the restrictions in individual cases. The Guidelines should be amended to clarify their application, preferably by removing reference to the application of restrictions by controllers. In particular, the Guidelines should clarify the difference between (1) a legislative measure which removes data subject rights and (2) a one-off refusal of the exercise of a right in a specific case, applying a proportionate restriction/exemption, which does not amount to a removal of rights.

2. Background to the Guidelines

On 4 May 2020, the Hungarian Government published a decree suspending the exercise of individuals' rights under Articles 15 to 22 GDPR in relation to the processing of personal data by public and private entities for the purpose of the fight against COVID 19. The suspension is to last until the "end of the state of danger." Further, the decree restricted the rights under Articles 77 to 79 GDPR to lodge complaints or seek judicial remedies. There is no indication of when the Hungarian government will reinstate the rights.

The Hungarian Civil Liberties Union and other civil society organisations raised a complaint with the EU Commission on the basis that the suspension and restrictions are incompatible with Hungary's obligations under the EU Treaty and EU law. The complaint stated that the decree (1) did not reference Article 23 GDPR; (2) did not amount to a "legislative measure" and (3) failed to meet the requirement that a measure

¹ CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 80 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at <http://www.informationpolicycentre.com/>. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

² [Guidelines 10/2020 on restrictions under Article 23 GDPR - version for public consultation](#)

³ As per footnote 4 of the Guidelines, the notion of "controller" also covers the notion of "processor" where applicable.

under Article 23 must “respect the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard public health.”

On 11 May 2020, the Hungarian Civil Liberties Union wrote to the EDPB asking it to advise the EU Commission on the issue in accord with Article 70(1)(b) GDPR. In its response, the EDPB issued a letter on 3 June 2020 noting that only the EU Commission can take legal steps against a Member State.

On 2 June 2020, the EDPB also issued a statement (Statement) on restrictions on data subject rights in connection to the state of emergency in Member States.⁴ The Statement reiterates the conditions applicable to Article 23 restrictions and includes the following paragraph 15:

“The EDPB takes the view that restrictions adopted in the context of a state of emergency suspending or postponing the application of data subject rights and the obligations incumbent to controllers and processors, without any clear limitation in time, would equate to a de facto blanket suspension of those rights and would not be compatible with the essence of the fundamental rights and freedoms. Moreover, the handling of a request to exercise the rights of data subjects, for instance concerning the right to object under Article 21 of the GDPR, must be processed timely to be meaningful and effective. Therefore, in this context, the postponement or suspension - without any specific limit in time - of the handling, by the controller, of the data subject requests would amount to a complete obstacle against the exercise of the rights themselves.”

The Statement also included a commitment for the EDPB to issue more comprehensive guidelines on the implementation of Article 23 GDPR. The Guidelines are the promised comprehensive guidelines. As would be anticipated, given the background, the Guidelines are primarily aimed at the EU Commission, Member States and, to a lesser extent, to DPAs. The target audience is not controllers.

3. Structure of the Guidelines and intended Audience

The Guidelines are not aimed at controllers. Most of the material in the Guidelines addresses the implementation of Article 23 GDPR by Member States and the circumstances under which rights can be suspended. However, at some points it strays into material on the application of restrictions/exemptions which then conflates guidance to Member States with guidance to controllers.

We understand the background which has given rise to these Guidelines. We wholly support the emphasis placed by the EDPB in its Statement on the importance of necessity and proportionality in drafting and providing for restrictions on individual rights in national legislation. We support the position taken by the EDPB in its Statement and support the importance attached to respecting individual rights. We agree with the EDPB that a general suspension of rights cannot be viewed as compatible with Article 23 GDPR. Nevertheless, we consider that the Guidelines as drafted are confusing and unhelpful to controllers and individuals. We would urge the EDPB to re-draft and re-name the document without undermining its central message.

⁴ [Statement on restrictions on data subject rights in connection to the state of emergency in Member States](#)

The Guidelines are a novel form of publication by the EDPB. They are unlike any other EDPB documents in being addressed primarily to Member States, and, to a lesser extent, DPAs. Controllers and individuals are not versed in these distinctions and will inevitably find the Guidelines confusing. CIPL members are among the most sophisticated organisations, but several of them struggled to respond to the request for comments on the consultation.

CIPL notes that only limited paragraphs in the Guidelines apply to controllers. The way the Guidelines are framed means that there can appear to be a conflation of the advice which applies to controllers with that which applies to Member States. For example, paragraph 63 moves from an assessment of the requirements of Article 23 to consider the application of a restriction by a controller in a particular case. This conflates the nature of a restriction with the application of a restriction. The application of a restriction will be fact-sensitive. It will depend on the specific restriction under consideration, the proper balance of proportionality and the interest to be protected.

CIPL submits that the limited guidance to controllers in the Guidelines should be removed and the document should be re-named appropriately, for example “Guidelines for Member States and Supervisory Authorities on restrictions under Article 23 GDPR.”

If the EDPB considers it is appropriate to issue additional guidance to controllers on the application of restrictions/exemptions, such guidance should be limited to the provision of general guidance on the proper approach to the application of restrictions/exemptions. Detailed specific guidance on the application of exemptions in national law is a matter for DPAs.

Alternatively, if the EDPB continues to aim to include guidance to Member States, to DPAs and to controllers in one document, the advice issued to the three different audiences should be clearly differentiated so those using the Guidelines can see clearly which part of the Guidelines apply to them.

4. Distinction between the application of restrictions under Article 23 and application of exemptions under national law

As noted above, CIPL considers this a critical distinction to be drawn. Where restrictions apply under national law, the pattern is that a controller may, in reliance on a relevant restriction, legitimately refuse the exercise of a data subject right, based on facts as they apply at the time when the individual seeks to exercise the right. As such, the individual’s rights are not removed, withdrawn or downgraded. There is no barrier to the subsequent exercise of the right. There is the possibility, accepted in Article 12(5) GDPR, that where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either refuse the request or charge a reasonable fee. However, a controller cannot suspend the operation of rights or forbid an individual from exercising those rights. This can only be done by a legislative or other legal act of the Member State. It follows that paragraphs 73 to 75 of the Guidelines are not applicable to the application of restrictions by controllers. Controllers cannot apply an on-going restriction in respect of individual rights.

The distinction between the legislative framing of a restriction and the application of an exemption was considered by the UK courts in *R (Open Rights and Others) v the Secretary of State for the Home*

*department and the Department of Culture Media and Sport.*⁵ The claimants challenged the lawfulness of an exemption in the 2018 UK Data Protection Act on the grounds that it is contrary to Article 23 GDPR and incompatible with Articles 7 and 8 of the EU Charter of Fundamental Rights.

The exemption applies to the rights in Articles 13 to 15, 17 to 18, and 21 and Article 5 provisions to the extent they correspond to those rights and applies where:

- The purpose of the processing is the maintenance of effective immigration control or the investigation or detection of activities that would undermine the maintenance of effective immigration control; and
- The exercise of the relevant right would be likely to prejudice the purposes of the processing.

The Court considered the exemption in the light of CJEU and UK case law and the tests of necessity, proportionality and foreseeability. The Court drew a distinction between cases where the legislation itself constituted or required an interference with rights and those where the legislation did not do so.⁶ In the former, it accepted a test of strict necessity was imposed on the State but the Court noted that the exemption in question did not of itself restrict individual rights.⁷ The Court took into account the context in which the exemption was exercised, noting that under existing case law, the prejudice test “must mean a real possibility of prejudice”⁸ and the other safeguards in the UK Data Protection Act and the GDPR.

CIPL submits that this distinction between the terms of a restriction as implemented by a Member State as opposed to the application of an exemption on a case-by-case basis by a controller is a central and critical one which should be reflected throughout the Guidelines.

Furthermore, restrictions under Article 23 GDPR shall not be conflated with other GDPR provisions, such as Article 89(2) GDPR, that already enables EU or a Member State law to restrict some individual rights under Articles 15, 16, 18 and 21 GDPR to the extent necessary for scientific, historical research or statistical purposes. Several Member States have already adopted such laws to facilitate scientific research, either in pre-GDPR research laws or post GDPR, relying on Article 89(2) GDPR.

5. Guidelines to Member States

CIPL suggests the following issues be considered when finalising Guidelines to Member States.

Article 23 provides for an element of a margin of appreciation for Member States in their areas of activity concerned by restrictions and the extent, nature and terms of those restrictions. In relation to the areas of activity covered, CIPL recognises and respects the realities of national cultural differences. Nevertheless, CIPL would strongly advocate an increase in discussions and exchanges between Member States with the aim of building consensus and eventually an increased convergence in the nature and range of restrictions they adopt. A divergence in the nature and scope of restrictions could potentially have an impact on the single market.

⁵ [England and Wales High Court \[2019\] 2562](#)

⁶ The Court referred to [Opinion 1/15](#) and [Tele2 Sverige AB v Post-Och Telestyrelsen](#).

⁷ See paragraph 45 of the Court decision.

⁸ See paragraph 49 of the Court decision.

We would also submit that a clear distinction should be drawn between those cases in which Member State law removes, limits or restricts individuals' rights and those cases in which the legislation provides for possible limitations on such rights by controllers on a specific case-by-case basis. In the former case, we agree that such legislation must be subject to the test of strict necessity and be time limited. In other cases, where a restriction has been properly embodied in national law, subject to safeguards, and embeds proportionality tests such as tests of necessity and prejudice, the necessity test to be applied by the controller on a specific case-by-case basis is one of ordinary proportionality.

CIPL fully agrees that in case of a restriction imposed by a Member State, once such a blanket restriction is lifted, some form of notice should be provided to individuals so they are aware that their proper rights have been restored.⁹ This obligation however cannot be placed on controllers. CIPL considers this should be an obligation on either the Member State or the DPA as part of the obligation to ensure individuals are made aware of their rights. As noted above, controllers cannot withdraw or restrict individual rights in time. An individual is entitled to continue to exercise rights subject to Article 12 potential responses.

6. Guidelines to Controllers

As noted earlier, we submit that guidance to controllers would be better in a separate document. In any event, there are a number of points we consider are important in any such guidance.

Guidance to controllers should make clear that Article 23 is not directly applicable to them and they cannot rely on it directly. Controllers should comply with applicable national law on restrictions unless and until such national laws are challenged and found to be non-compliant with the GDPR. This could leave open the possibility that, in a case such as the Hungarian decree, a controller could exercise discretion to grant individuals notice, access and other rights even though the individuals cannot enforce these. We recognise however that the guidance would have to make clear that the controller would have no discretion where the national law forbids access, notice, etc.

As per footnote 4 of the current Guidelines, the notion of "controller" also covers the notion of "processor" where applicable. Any separate guidance should make clear that it is addressed to both controllers and processors by making this more visible in the body of the text (rather than in a footnote).

The guidance should also recognise that restrictions may be applied in a vast range of circumstances. We provide some examples below in relation to data subject rights.

6.1 *Mandatory restrictions*

The guidance should confirm that controllers complying with explicit legal requirements to apply restrictions under national law (including an enactment, a rule of law or the order of a court) do not need to assess the necessity and proportionality of a restriction. As an example, a controller which has supplied information to a policing or other criminal investigative agency could be forbidden by law from disclosing that fact to the concerned individual (ex officio or in response to an individual access request), because

⁹ See paragraph 88 of the Guidelines.

to do so means committing a tipping off offence.¹⁰ Controllers should not be penalised or held otherwise liable for complying with such requirements. Member States have a wide discretion under Article 23(1)(e) to determine matters of general public interest. In some cases, the law may be unclear or the controller possibly subject to conflicting requirements. Controllers should not be required to navigate between legislative terms, or be held in any way liable where inconsistencies in law emerge.

6.2 Rights refusal in reliance on third party evidence

Further, restrictions may have to be applied in reliance on the judgement of a party with expertise in a particular area. As an example, an educational establishment may hold records about a child's behaviour which have been provided by a clinical adviser such as a child psychologist. A parent with parental rights may seek to exercise the child's right of access in respect of such data. In such a case, the controller will have to exercise a judgement as to whether to give or withhold the data but in doing so may have to rely on the judgement of another (the relevant expert). We would advocate that proper procedures should be put in place to address such cases (e.g. the use of standard forms signed off by the appropriate person), but in principle controllers should be entitled to rely in good faith on the specific expertise of others, subject to following proper procedures and checking, as far as possible, that any restriction is proportionate.

6.3 Discretionary decisions

In other cases, of course controllers must exercise their own judgement and have an element of discretion as to whether or not to apply restrictions. As a general statement, CIPL agrees that in such cases, controllers should ensure that any restrictions in national law are applied:

- In accordance with national law;
- On the basis of evidence relevant to the case;
- Taking account of any appropriate expert input e.g. on the consequences of disclosure of information to the mental health of an individual; and
- Applying the proper tests of proportionality.

Overall, however, given the range of exemptions which may apply, the varied nature of controllers and the many fact patterns which may be applicable, CIPL considers that EDPB guidance is unlikely to be able to go beyond such general advice. In this regard, it considers that the very specific suggestions in the Guidance are misconceived. For example, in paragraph 65, the advice that, after an initial stage of an investigation, individuals should receive a specific data protection notice. The question of when and how notices that rights have been restricted should be provided in any case will depend on the facts and the circumstances. As an example, a controller could legitimately restrict the supply of information to an individual who has been guilty of domestic violence towards family members, for as long as the supply of such information would involve real risk to the family members. In addition, as stated by the Article 29 Working Party in its opinion on whistleblowing schemes, "[u]nder no circumstances can the person accused in a whistleblower's report obtain information about the identity of the whistleblower from the

¹⁰ Disclosing this fact is a tipping off offence because it may jeopardise an on-going investigation, or put other individuals at risk.

scheme on the basis of the accused person's right of access, except where the whistleblower maliciously makes a false statement. Otherwise, the whistleblower's confidentiality should always be guaranteed."¹¹

Given the huge range of issues which arise in practice in applying restrictions or exemptions, CIPL would urge the EDPB to carry out consultations with controllers and organisations representing individuals before it drafts any specific guidance on the exercise of individual rights in practice.

6.4 Additional obligations

Any guidance to controllers should not be used to impose additional procedural requirements. In particular:

- Controllers have no legal obligation under the GDPR to notify DPOs of all restrictions.¹² In many cases, restrictions will be applied as a result of the expert judgement of specialists in the area. This would apply to clinical decisions, social work or educational decisions, many anti-money laundering, investigative or regulatory decisions. The important point is that those who make the decisions are properly trained in the data protection issues and follow proper procedures to apply the right balance. CIPL agrees that, in difficult or finely balanced cases, the expertise of the DPO will be invaluable but it is not a requirement that the DPO is always involved.
- Controllers have no obligation under the GDPR to document the reasons for restrictions in all cases.¹³ This is usually good practice, particularly in a difficult case where the controller has had to make a balanced judgment, however it is not part of the records required under Article 30 GDPR. It would be inappropriate to record detailed information for example where there is a legal obligation to refuse a request. In other cases, records will be made in the relevant action files, for example a clinical decision not to disclose information to a patient, a restriction recorded on an investigation, or a claim of legal professional privilege. There is no requirement to duplicate such records.
- Controllers should not be required to conduct a necessity and proportionality assessment during the application of a restriction when complying with an explicit legal requirement to apply restrictions under national law.
- More generally, the EDPB should refrain from creating indefinite and impractical further compliance obligations on controllers, e.g., by requiring to keep a record of the situations in which restrictions are lifted; by requiring to continue to monitor cases where documents have been withheld on the basis of privilege or where notice cannot be legally provided further to lawful gag orders.

¹¹ [Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime.](#)

¹² See paragraph 67 of the Guidelines.

¹³ See paragraph 66 of the Guidelines.

7. Guidelines to DPAs

CIPL does not represent any DPAs among its membership. We have only limited comments on the aspects of the Guidelines as they apply to DPAs. Paragraph 71 of the Guidelines states that, as part of the adoption of restrictions by a Member state in the legislative or regulatory process, a DPA could ask for a DPIA under Article 35. CIPL's understanding is that such a DPIA can only be required from a controller. Under the circumstances where the Member State is framing a legislative measure dealing with a restriction there is no certainty that the restriction will be applied by any organ of the State acting as controller. It is more likely to apply to controllers who are not under the control of the State. The Guidelines should make this point clear. CIPL also suggests that before a law restricting individual rights is adopted, a (joint) non-binding opinion of the DPA and the public authority representing the relevant public interest at hand is requested and considered.

Conclusion

CIPL is grateful for the opportunity to provide feedback and respond to the EDPB's Consultation on restrictions under Article 23 GDPR. We appreciate the EDPB's consideration of various stakeholders' views on these Guidelines. If you would like to discuss any of the comments or recommendations in this response, please contact Bojana Bellamy, bbellamy@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; or Markus Heyder at mheyder@huntonAK.com.